What is claimed is:

1. A method for use with a stateful packet processing device of a computer network for mitigating effects of a network overload against said device, said method operable to free memory used to store information about communications sessions managed by said device, said method comprising the steps of:

classifying session cache entries made in memory into different cache classes, according to one or more characteristics of those entries;

determining when said device is under network overload;

selecting session cache entries for deletion and deleting them thereby freeing associated memory when said device is under network overload;

determining when sufficient memory has been freed, such that said cache entries are no longer deleted.

2. The method of Claim 1, wherein said characteristics for said step of classifying are selected from the group consisting of: whether the session is dropped by the device, whether the session is audited by the device, IP protocol of the session, ICMP type and code used in the session, TCP ports used in the session, UDP ports used in the session, and whether the session is a half-open TCP session.

3. The method of Claim 1, wherein certain of said characteristics of the session may be identified as "any", wherein any session matches a particular criterion for classification.

4. The method of Claim 1, wherein predefined cache classes are selected from the group consisting of:

dropped and unaudited sessions, dropped and audited sessions, ICMP sessions, and half-open TCP sessions.

5. The method of claim 4, wherein the predefined cache classes are assigned a priority for deletion.

6. The method of Claim 1, wherein the device is considered to be under network overload when the amount of memory used for session cache entries exceeds a configurable trigger threshold.

7. The method of Claim 6, wherein a sufficient amount of memory has been freed when the amount of memory used for session cache entries falls below a configurable floor threshold.

8. The method of Claim 4, wherein a memory usage threshold is configurable for each predefined cache class.

9. The method of Claim 8, wherein said step of selecting and deleting includes the steps of:

retrieving from a database the amount of memory used to store session cache entries for each cache class ;

recognizing each cache class whose memory usage exceeds an associated memory usage threshold;

ordering each cache class according to its deletion priority;

selecting for deletion according to said ordering step some fraction of entries of a given cache class if said deletion brings said total cache memory usage below said floor, wherein, otherwise, all entries of said given class are selected for deletion; and

continuing said step of selecting for deletion until it is determined that either deleting all the entries selected for deletion would bring the total cache memory usage below the floor threshold, or all entries in all defined cache classes have been selected for deletion.

10. The method of Claim 9, wherein said step of ordering includes ordering cache classes whose memory usage does not exceed said associated memory usage threshold.

11. The method of Claim 9, wherein configuration data for the thresholds may be supplied in a normalized fashion and be adaptively applied to the device, depending on the amount of memory on the device.

12. An apparatus for use with a stateful packet processing device of a computer network for mitigating effects of a network overload against said device, said apparatus operable to free memory used to store information about communications sessions managed by said device, said system comprising:

a classification component operable to determine, for each session cache entry, the cache class to which that entry belongs according to one or more characteristics of the entry;

a memory management database for tracking the amounts of memory used for each category of entry, as well as for tracking the total amount of memory used for all entries;

a pruning component that is used to select and delete entries; and

a processor for determining when said device is experiencing network overload and selecting specific cache session entries for deletion until sufficient memory has been freed.

13. The apparatus of Claim 12, wherein information kept in the memory management database is updated each time a new cache entry is created or deleted by the device.

14. The apparatus of Claim 12, wherein said characteristics for said step of classifying are selected from the group consisting of: whether the session is dropped by the device, whether the session is audited by the device, IP protocol of the session, ICMP type and code used in the session, TCP ports used in the session, UDP ports used in the session, and whether the session is a half-open TCP session.

15. The apparatus of Claim 14, wherein certain of said characteristics of the session may be identified as “any”, wherein any session matches a particular criterion for classification.

16. The apparatus of Claim 12, wherein predefined cache classes are selected from the group consisting of:

dropped and unaudited sessions, dropped and audited sessions, ICMP sessions, and half-open TCP sessions.

17. The apparatus of claim 16, wherein the predefined cache classes are assigned a priority for deletion.

18. The apparatus of Claim 16, wherein a memory usage threshold is configurable for each predefined cache class.

19. The apparatus of Claim 12, wherein the pruning mechanism selects entries for deletion by:

retrieving from a database the amount of memory used to store session cache entries for each cache class ;

recognizing each cache class whose memory usage exceeds an associated memory usage threshold;

ordering each cache class according to its deletion priority;

selecting for deletion according to said ordering step some fraction of entries of a given cache class if said deletion brings said total cache memory usage below a floor threshold, wherein, otherwise, all entries of said given class are selected for deletion; and

continuing said step of selecting for deletion until it is determined that either deleting all the entries selected for deletion would bring the total cache memory usage below the floor threshold, or all entries in all defined cache classes have been selected for deletion.

20. The apparatus of Claim 19, wherein said step of ordering includes cache classes whose memory usage does not exceed said associated memory usage threshold.

21. The apparatus of Claim 19, wherein the pruning mechanism operates by making only one pass through a list of session cache entries in said device.

22. The apparatus of Claim 12, wherein a trigger threshold and floor threshold corresponding to said total memory usage are adjustably configurable.

23. The system of Claim 12, wherein the memory usage statistics are collected using the Simple Network Management Protocol (SNMP).

24. The apparatus of Claim 12, wherein the pruning mechanism, when it has to delete some fraction of the entries in a given cache class, approximates the fraction b/t (where b is the total number of bytes of memory that must be freed and t is the total number of bytes of memory used to hold session cache entries for that cache class) with another fraction p/q, where p >=1 and q is likely to be small relative to the total number of cache entries in that class; and then frees p entries out of every q entries in that cache class on the list of session cache entries.

25. A cache management system used in connection with session-type packet processing devices of a computer network, said system comprising:

a memory management database for storing communication traffic classification and memory threshold values;

a memory monitor for tracking overall memory usage and determining when said memory threshold values stored in said memory management database are reached;

a cache classifier used to determine a class into which a given session of communications traffic falls; and

a pruner mechanism for selecting and pruning selected sessions of said packet processing device in accordance with said communication traffic classification and memory thresholds programmed in said memory management database when said memory threshold value is reached.

26. The system of Claim 25 wherein said prune selector is operable to selectively prune sessions of an ordered overlimit class if the memory used by said class is greater than the difference between a global ceiling threshold and a global floor threshold.

27. The system of Claim 26, wherein said prune selector is operable to prune all sessions of said overlimit class if the memory used by said class is less than the difference between said global ceiling threshold and said global floor threshold.

28. The system of Claim 27, wherein a next highest priority class is examined to determine if memory used by said class is greater than a remaining difference between said global ceiling threshold and said global floor threshold, said next highest priority class being selectively pruned if said difference is greater than said remaining difference.

29. The system of Claim 28, wherein said prune selector is operable to prune all sessions of said next highest priority class if the memory used by said class is less than said remaining difference.

30. The system of Claim 25, wherein said devices are selected form the group consisting of: network firewalls, routers, switches and hosts.